

PCT/JP 99/00292

日 本 国 特 許 庁

22.02.99

PATENT OFFICE
JAPANESE GOVERNMENT

REC'D 08 APR 1999

09/381996 KU

WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

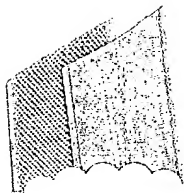
1998年 2月 9日

出 願 番 号
Application Number:

平成10年特許願第027572号

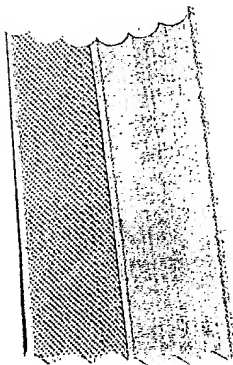
出 願 人
Applicant(s):

松下電器産業株式会社



PRIORITY DOCUMENT

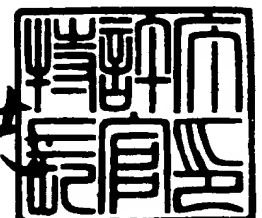
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)



1999年 3月26日

特 許 庁 長 官
Commissioner,
Patent Office

伴佐山 建志



出証番号 出証特平11-3017393

【書類名】 特許願

【整理番号】 2054500013

【提出日】 平成10年 2月 9日

【あて先】 特許庁長官殿

【国際特許分類】 G11B 20/00

【発明の名称】 録画装置および再生装置

【請求項の数】 27

【発明者】

 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

 【氏名】 山田 正純

【発明者】

 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

 【氏名】 飯塚 裕之

【発明者】

 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

 【氏名】 武知 秀明

【発明者】

 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

 【氏名】 後藤 昌一

【特許出願人】

 【識別番号】 000005821

 【氏名又は名称】 松下電器産業株式会社

【代理人】

 【識別番号】 100092794

 【弁理士】

【氏名又は名称】 松田 正道

【電話番号】 06 397-2840

【手数料の表示】

【予納台帳番号】 009896

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9006027

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 録画装置および再生装置

【特許請求の範囲】

【請求項 1】 映像および／または音のデータを入力するとともに、前記映像および／または音のデータをスクランブルするためのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、

前記スクランブル鍵を暗号化するための暗号化鍵を発生する暗号化鍵発生手段と、

前記暗号化鍵発生手段が発生した暗号化鍵を格納し、その後、その暗号化鍵が所定の条件に合えば、その暗号化鍵を消去する格納手段と、

前記スクランブル手段からのスクランブル鍵を入力するとともに、前記暗号化鍵発生手段からの前記暗号化鍵を入力し、その暗号化鍵で前記スクランブル鍵を暗号化する鍵暗号化手段と、

前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵を暗号化した暗号化鍵との対応関係情報を生成する対応関係情報生成手段と、

前記スクランブル手段からのスクランブルされた映像および／または音のデータ、前記鍵暗号化手段からの暗号化されたスクランブル鍵、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを

備えたことを特徴とする録画装置。

【請求項 2】 前記所定の条件とは、前記暗号化鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項 1 記載の録画装置。

【請求項 3】 前記対応関係情報とは、前記スクランブル手段が前記映像および／または音のデータを入力した日時、前記スクランブル手段が前記スクランブル鍵で前記映像および／または音のデータをスクランブルした日時、前記暗号化鍵発生手段が前記暗号化鍵を発生した日時、前記格納手段が前記暗号化鍵を格納した日時、前記鍵暗号化手段が前記暗号化鍵で前記スクランブル鍵を暗号化した日

時、または、前記記録手段が前記所定の記録媒体に前記スクランブルされた映像および／または音のデータを記録した日時で対応付けられた情報であることを特徴とする請求項 1 または 2 記載の録画装置。

【請求項 4】前記所定の条件とは、前記スクランブルされた映像および／または音のデータの再生のさいに、前記暗号化鍵の利用された回数が、所定の回数をを超えることを意味することを特徴とする請求項 1 記載の録画装置。

【請求項 5】前記スクランブル鍵を発生するスクランブル鍵発生手段を備え、前記スクランブル手段は、前記スクランブル鍵発生手段から前記スクランブル鍵を入力することを特徴とする請求項 1 から 4 のいずれかに記載の録画装置。

【請求項 6】前記スクランブル手段は、放送局からの前記スクランブル鍵を入力し、そのスクランブル鍵を利用することを特徴とする請求項 1 から 4 のいずれかに記載の録画装置。

【請求項 7】請求項 1 から 6 のいずれかに記載の所定の記録媒体からの、請求項 1 から 6 のいずれかに記載の前記対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応する暗号化鍵を特定し、請求項 1 から 6 のいずれかに記載の格納手段のなかの前記暗号化鍵を検索して取得する暗号化鍵取得手段と、

前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、暗号化されたスクランブル鍵を入力するとともに、前記暗号化鍵取得手段からの暗号化鍵を入力し、その暗号化鍵で前記暗号化された前記スクランブル鍵の暗号化を解く鍵暗号化解読手段と、

前記所定の記録媒体からの、スクランブルされた映像および／または音のデータを入力するとともに、前記鍵暗号化解読手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを

備えたことを特徴とする再生装置。

【請求項 8】映像および／または音のデータを入力するとともに、前記映像および／または音のデータをスクランブルするためのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスク

ランブル手段と、

前記スクランブル鍵を暗号化するための暗号化鍵を発生する暗号化鍵発生手段と、

前記暗号化鍵発生手段が発生した暗号化鍵を格納する格納手段と、

前記スクランブル手段からのスクランブル鍵を入力するとともに、前記暗号化鍵発生手段からの前記暗号化鍵を入力し、その暗号化鍵で前記スクランブル鍵を暗号化する鍵暗号化手段と、

前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵を暗号化した暗号化鍵との対応関係情報を生成する対応関係情報生成手段と、

前記スクランブル手段からのスクランブルされた映像および／または音のデータ、前記鍵暗号化手段からの暗号化されたスクランブル鍵、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを

備えたことを特徴とする録画装置。

【請求項 9】前記対応関係情報とは、前記スクランブル手段が前記映像および／または音のデータを入力した日時、前記スクランブル手段が前記スクランブル鍵で前記映像および／または音のデータをスクランブルした日時、前記暗号化鍵発生手段が前記暗号化鍵を発生した日時、前記格納手段が前記暗号化鍵を格納した日時、前記鍵暗号化手段が前記暗号化鍵で前記スクランブル鍵を暗号化した日時、または、前記記録手段が前記所定の記録媒体に前記スクランブルされた映像および／または音のデータを記録した日時で対応付けられた情報であることを特徴とする請求項 8 記載の録画装置。

【請求項 10】前記スクランブル鍵を発生するスクランブル鍵発生手段を備え、前記スクランブル手段は、前記スクランブル鍵発生手段から前記スクランブル鍵を入力することを特徴とする請求項 8 または 9 記載の録画装置。

【請求項 11】前記スクランブル手段は、放送局からの前記スクランブル鍵を入力し、そのスクランブル鍵を利用することを特徴とする請求項 8 または 9 記載の録画装置。

【請求項 12】請求項 8 から 11 のいずれかに記載の所定の記録媒体からの、請求項 8 から 11 のいずれかに記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応する暗号化鍵を特定し、さらに、その暗号化鍵が所定の条件に合うかどうかを判定し、合致する場合は、その暗号化鍵を、請求項 8 から 11 のいずれかに記載の格納手段から取り出し、合致しない場合は、その暗号化鍵を前記格納手段から取り出さない暗号化鍵取得手段と、

前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、暗号化されたスクランブル鍵を入力するとともに、前記暗号化鍵取得手段からの暗号化鍵を入力し、その暗号化鍵で前記暗号化された前記スクランブル鍵の暗号化を解く鍵暗号化解読手段と、

前記所定の記録媒体からの、スクランブルされた映像および／または音のデータを入力するとともに、前記鍵暗号化解読手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを

備えたことを特徴とする再生装置。

【請求項 13】前記所定の条件とは、請求項 8 から 11 のいずれかに記載の格納手段に、前記暗号化鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項 12 記載の再生装置。

【請求項 14】前記所定の条件とは、前記スクランブルされた映像および／または音のデータの再生のさいに、前記暗号化鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項 12 記載の再生装置。

【請求項 15】映像および／または音のデータをスクランブルするためのスクランブル鍵を発生するスクランブル鍵発生手段と、

前記スクランブル鍵発生手段が発生したスクランブル鍵を格納し、その後、そのスクランブル鍵が所定の条件に合えば、そのスクランブル鍵を消去する格納手段と、

前記映像および／または音のデータを入力するとともに、前記スクランブル鍵発生手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および

／または音のデータをスクランブルするスクランブル手段と、

前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵との対応関係情報を生成する対応関係情報生成手段と、

前記スクランブル手段からのスクランブルされた映像および／または音のデータ、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを

備えたことを特徴とする録画装置。

【請求項16】前記所定の条件とは、前記スクランブル鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項15記載の録画装置。

【請求項17】前記対応関係情報とは、前記スクランブル手段が前記映像および／または音のデータを入力した日時、前記スクランブル手段が前記スクランブル鍵で前記映像および／または音のデータをスクランブルした日時、前記スクランブル鍵発生手段が前記スクランブル鍵を発生した日時、前記格納手段が前記スクランブル鍵を格納した日時、または、前記記録手段が前記所定の記録媒体に前記スクランブルされた映像および／または音のデータを記録した日時で対応付けられた情報であることを特徴とする請求項15または16記載の録画装置。

【請求項18】前記所定の条件とは、前記スクランブルされた映像および／または音のデータの再生のさいに、前記暗号化鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項15記載の録画装置。

【請求項19】請求項15から18のいずれかに記載の所定の記録媒体からの、請求項15から18のいずれかに記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応するスクランブル鍵を特定し、請求項15から18のいずれかに記載の格納手段のなかの前記スクランブル鍵を検索して取得するスクランブル鍵取得手段と、

前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、前記スクランブルされた映像および／または音のデータを入力するとともに、前記スクランブル鍵取得手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／ま

たは音のデータのスクランブルを解除するスクランブル解除手段とを
備えたことを特徴とする再生装置。

【請求項 20】映像および／または音のデータをスクランブルするためのスクランブル鍵を発生するスクランブル鍵発生手段と、

前記スクランブル鍵発生手段が発生したスクランブル鍵を格納する格納手段と

、
前記映像および／または音のデータを入力するとともに、前記スクランブル鍵発生手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、

前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵との対応関係情報を生成する対応関係情報生成手段と、

前記スクランブル手段からのスクランブルされた映像および／または音のデータ、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを

備えたことを特徴とする録画装置。

【請求項 21】前記対応関係情報とは、前記スクランブル手段が前記映像および／または音のデータを入力した日時、前記スクランブル手段が前記スクランブル鍵で前記映像および／または音のデータをスクランブルした日時、前記スクランブル鍵発生手段が前記スクランブル鍵を発生した日時、前記格納手段が前記スクランブル鍵を格納した日時、または、前記記録手段が前記所定の記録媒体に前記スクランブルされた映像および／または音のデータを記録した日時で対応付けられた情報であることを特徴とする請求項 20 記載の録画装置。

【請求項 22】請求項 20 または 21 記載の所定の記録媒体からの、請求項 20 または 21 記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応するスクランブル鍵を特定し、さらに、そのスクランブル鍵が所定の条件に合うかどうかを判定し、合致する場合は、そのスクランブル鍵を、請求項 20 または 21 記載の格納手段から取り出し、合致しない場合は、そのスクランブル鍵を前記格納手段から取り出さないスクランブル鍵取得手段と、

前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、スクランブルされた映像および／または音のデータを入力するとともに、前記スクランブル鍵取得手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置。

【請求項 23】前記所定の条件とは、請求項 20 または 21 記載の格納手段に、前記スクランブル鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項 22 記載の再生装置。

【請求項 24】前記所定の条件とは、前記スクランブルされた映像および／または音のデータの再生のさいに、前記スクランブル鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項 22 記載の再生装置。

【請求項 25】前記記録手段が前記スクランブル手段からのスクランブルされた映像および／または音のデータを、前記所定の記録媒体に記録するさい、前記データの記録に対する課金を課す課金手段を備えたことを特徴とする請求項 1 から 6 のいずれか、または、請求項 8 から 11 のいずれか、または、請求項 15 から 18 のいずれか、または、請求項 20 から 21 のいずれかに記載の録画装置。

【請求項 26】前記所定の記録媒体は、ビデオテープであることを特徴とする請求項 1 から 6 のいずれか、または、請求項 8 から 11 のいずれか、または、請求項 15 から 18 のいずれか、または、請求項 20 から 21 のいずれかに記載の録画装置。

【請求項 27】前記所定の記録媒体は、ハードディスクであることを特徴とする請求項 1 から 6 のいずれか、または、請求項 8 から 11 のいずれか、または、請求項 15 から 18 のいずれか、または、請求項 20 から 21 のいずれかに記載の録画装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、著作権等により再生についての期間や回数が制限された、映像およ

び／または音のデータを録画する録画装置と、その映像および／または音のデータを再生する再生装置とに関するものである。

【0002】

【従来の技術】

現在、著作権保護の対象となっている映画や音楽等のAVデータは、ビデオテープ等に格納されている。ユーザは、そのようなビデオテープ等を有料で貸し出すレンタル店を通じて、例えば1週間というような所定の期間のみビデオテープ等を借り、それを再生することによって、映画や音楽等を鑑賞することができる。

【0003】

他方、上述したビデオテープ等のレンタルのシステムとは別に、デジタル技術や暗号化技術の進歩等から、放送局からの映画や音楽等の番組を通信衛星を介して入力し、その番組をスクランブルしてビデオテープ等に録画し、再生する録画再生装置として、以下のものが考えられている。

【0004】

図7に、このような従来の録画再生装置のブロック図を示す。

【0005】

受信復調手段1は、衛星放送の、デジタルの映像データ、音データ、EMM（個別情報）、ECM（番組情報）および暗号化された放送スクランブル鍵Ksを入力し、第1DMUX2は、受信復調手段1からの映像データ、音データ、EMM、ECMおよび放送スクランブル鍵Ksを分離する。そして、EMM解読手段3は、第1DMUX2からのEMMを入力するとともに、ユーザID鍵Kmを入力し、そのユーザID鍵KmでEMMを解読してワーク鍵Kwを生成する。ECM解読手段4は、EMM解読手段3からのワーク鍵Kwを入力するとともに、第1DMUX2からのECMおよび暗号化された放送スクランブル鍵Ksを入力し、ワーク鍵KwでECMを解読して、暗号化された放送スクランブル鍵Ksを復元する。

【0006】

その後、放送デスクランブル手段5は、ECM解読手段4からの放送スクラン

ブル鍵 K_s を入力するとともに、第1 DMUX 2からの、スクランブルされたAVデータを入力し、放送スクランブル鍵 K_s で、スクランブルされたAVデータをデスクランブルする。そして、放送デスクランブル手段5は、デスクランブルされたAVデータを、リアルタイムでAVデータを直接ディスプレイ21に表示させる場合に第1 DMUX 2に出力し、また、ビデオテープ20にAVデータを記録させる場合に記録スクランブル手段7に出力する。

【0007】

放送デスクランブル手段5がAVデータを第1 DMUX 2に出力する場合、第1 DMUX 2は、放送デスクランブル手段5からのAVデータを映像データと音データに分離して、映像データを映像デコーダ18に出力し、音データを音デコーダ19に出力する。そして、映像デコーダ18および音デコーダ19それぞれは、第1 DMUX 2からの映像データまたは音データを復号し、ディスプレイ21は、映像を表示し音を出力する。

【0008】

他方、放送デスクランブル手段5がAVデータを記録スクランブル手段7に出力する場合、記録スクランブル手段7は、放送デスクランブル手段5からのAVデータを入力するとともに、第1 鍵発生手段6からの記録スクランブル鍵 K_{ss} を入力し、その記録スクランブル鍵 K_{ss} で、AVデータをスクランブルする。その記録スクランブル鍵 K_{ss} によりスクランブルされたAVデータを K_{ss} (AVデータ) とする。

【0009】

それとともに、第2 鍵発生手段8は、記録スクランブル鍵 K_{ss} を暗号化するための暗号化鍵 K_c を発生し、鍵暗号化手段10は、第1 鍵発生手段6からの記録スクランブル鍵 K_{ss} を入力するとともに、第2 鍵発生手段8からの暗号化鍵 K_c を入力し、その暗号化鍵 K_c で記録スクランブル鍵 K_{ss} を暗号化する。その暗号化鍵 K_c により暗号化された記録スクランブル鍵 K_{ss} を K_c (K_{ss}) とする。

【0010】

そして、MUX 12は、記録スクランブル手段7からの K_{ss} (AVデータ)

と、鍵暗号化手段10からのKc (Kss) とを入力し、それらをビデオテープ20に記録する。

【0011】

そのビデオテープ20に記録されたKss (AVデータ) を再生する場合、先ず、第2DMUX13は、ビデオテープ20からのKss (AVデータ) と、Kc (Kss) とを入力して分離する。そして、鍵解読手段16は、第2DMUX13からのKc (Kss) を入力するとともに、第2鍵発生手段8からの暗号化鍵Kcを入力し、その暗号化鍵KcでKc (Kss) を解読して、記録スクランブル鍵Kssを復元する。さらに、再生デスクランブル手段17は、第2DMUX13からのKss (AVデータ) を入力するとともに、鍵解読手段16からの記録スクランブル鍵Kssを入力し、その記録スクランブル鍵KssでKss (AVデータ) をデスクランブルして、そのデスクランブルされたAVデータを第1DMUX2に出力する。

【0012】

最後に、第1DMUX2に出力されたAVデータは、リアルタイムにおける、ディスプレイ21の映像表示および音出力と同様にして、ディスプレイ21によって映像として表示され、また、音として出力される。

【0013】

【発明が解決しようとする課題】

ところで、上述したビデオテープ等のレンタルのシステムは、これからの多チャンネルデジタル放送時代においても、ユーザがその都度レンタル店に出向いてビデオテープ等を借りなければならないという点など、ユーザにとって相変わらず手間がかかり不便である。

【0014】

また、上述した従来の録画再生装置では、AVデータを一度ビデオテープ20に記録すると、第2鍵発生手段8からの暗号化鍵Kcを利用しさえすれば、そのAVデータは、いつでも、また、何度でも再生され、ディスプレイ21によって映像および／または音として出力される。このように、従来の録画再生装置では、映画や音楽等の著作権保護の対象となっているAVデータの有効再生期間や有

効再生回数には制限がないということになる。例えば、劇場放映直後の映画のように、特別な価値を有するＡＶデータが上述したような、再生の期間や回数について制限のない録画再生装置によって記録媒体に記録されると、そのＡＶデータの価値は半減する。つまり、放送局は、そのような特別な価値を有するＡＶデータを安心して放送することができない。

【0015】

本発明は、このような従来の録画再生装置は、ＡＶデータを記録媒体に記録すると、そのＡＶデータの有効再生期間や有効再生回数の制限を守らないという課題を考慮し、ＡＶデータを記録媒体に記録し、そのＡＶデータの有効再生期間や有効再生回数の制限を遵守する録画装置および再生装置を提供することを目的とするものである。

【0016】

【課題を解決するための手段】

請求項１の本発明は、映像および／または音のデータを入力するとともに、前記映像および／または音のデータをスクランブルするためのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、前記スクランブル鍵を暗号化するための暗号化鍵を発生する暗号化鍵発生手段と、前記暗号化鍵発生手段が発生した暗号化鍵を格納し、その後、その暗号化鍵が所定の条件に合えば、その暗号化鍵を消去する格納手段と、前記スクランブル手段からのスクランブル鍵を入力するとともに、前記暗号化鍵発生手段からの前記暗号化鍵を入力し、その暗号化鍵で前記スクランブル鍵を暗号化する鍵暗号化手段と、前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵を暗号化した暗号化鍵との対応関係情報を生成する対応関係情報生成手段と、前記スクランブル手段からのスクランブルされた映像および／または音のデータ、前記鍵暗号化手段からの暗号化されたスクランブル鍵、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置である。

【0017】

請求項 7 の本発明は、請求項 1 から 6 のいずれかに記載の所定の記録媒体からの、請求項 1 から 6 のいずれかに記載の前記対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応する暗号化鍵を特定し、請求項 1 から 6 のいずれかに記載の格納手段のなかの前記暗号化鍵を検索して取得する暗号化鍵取得手段と、前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、暗号化されたスクランブル鍵を入力するとともに、前記暗号化鍵取得手段からの暗号化鍵を入力し、その暗号化鍵で前記暗号化された前記スクランブル鍵の暗号化を解く鍵暗号化読手段と、前記所定の記録媒体からの、スクランブルされた映像および／または音のデータを入力するとともに、前記鍵暗号化読手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置である。

【0018】

請求項 8 の本発明は、映像および／または音のデータを入力するとともに、前記映像および／または音のデータをスクランブルするためのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、前記スクランブル鍵を暗号化するための暗号化鍵を発生する暗号化鍵発生手段と、前記暗号化鍵発生手段が発生した暗号化鍵を格納する格納手段と、前記スクランブル手段からのスクランブル鍵を入力するとともに、前記暗号化鍵発生手段からの前記暗号化鍵を入力し、その暗号化鍵で前記スクランブル鍵を暗号化する鍵暗号化手段と、前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵を暗号化した暗号化鍵との対応関係情報を生成する対応関係情報生成手段と、前記スクランブル手段からのスクランブルされた映像および／または音のデータ、前記鍵暗号化手段からの暗号化されたスクランブル鍵、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置である。

【0019】

請求項 12 の本発明は、請求項 8 から 11 のいずれかに記載の所定の記録媒体からの、請求項 8 から 11 のいずれかに記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応する暗号化鍵を特定し、さらに、その暗号化鍵が所定の条件に合うかどうかを判定し、合致する場合は、その暗号化鍵を、請求項 8 から 11 のいずれかに記載の格納手段から取り出し、合致しない場合は、その暗号化鍵を前記格納手段から取り出さない暗号化鍵取得手段と、前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、暗号化されたスクランブル鍵を入力するとともに、前記暗号化鍵取得手段からの暗号化鍵を入力し、その暗号化鍵で前記暗号化された前記スクランブル鍵の暗号化を解く鍵暗号化読手段と、前記所定の記録媒体からの、スクランブルされた映像および／または音のデータを入力するとともに、前記鍵暗号化読手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置である。

【0020】

請求項 15 の本発明は、映像および／または音のデータをスクランブルするためのスクランブル鍵を発生するスクランブル鍵発生手段と、前記スクランブル鍵発生手段が発生したスクランブル鍵を格納し、その後、そのスクランブル鍵が所定の条件に合えば、そのスクランブル鍵を消去する格納手段と、前記映像および／または音のデータを入力するとともに、前記スクランブル鍵発生手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵との対応関係情報を生成する対応関係情報生成手段と、前記スクランブル手段からのスクランブルされた映像および／または音のデータ、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置である。

【0021】

請求項 19 の本発明は、請求項 15 から 18 のいずれかに記載の所定の記録媒体からの、請求項 15 から 18 のいずれかに記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応するスクランブル鍵を特定し、請求項 15 から 18 のいずれかに記載の格納手段のなかの前記スクランブル鍵を検索して取得するスクランブル鍵取得手段と、前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、前記スクランブルされた映像および／または音のデータを入力するとともに、前記スクランブル鍵取得手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置である。

【0022】

請求項 20 の本発明は、映像および／または音のデータをスクランブルするためのスクランブル鍵を発生するスクランブル鍵発生手段と、前記スクランブル鍵発生手段が発生したスクランブル鍵を格納する格納手段と、前記映像および／または音のデータを入力するとともに、前記スクランブル鍵発生手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵との対応関係情報を生成する対応関係情報生成手段と、前記スクランブル手段からのスクランブルされた映像および／または音のデータ、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置である。

【0023】

請求項 22 の本発明は、請求項 20 または 21 記載の所定の記録媒体からの、請求項 20 または 21 記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応するスクランブル鍵を特定し、さらに、そのスクランブル鍵が所定の条件に合うかどうかを判定し、合致する場合は、そのスクランブル鍵を、請求項 20 または

21 記載の格納手段から取り出し、合致しない場合は、そのスクランブル鍵を前記格納手段から取り出さないスクランブル鍵取得手段と、前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、スクランブルされた映像および／または音のデータを入力するとともに、前記スクランブル鍵取得手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置である。

【0024】

【発明の実施の形態】

以下に、本発明の実施の形態を図面を参照して説明する。

【0025】

(実施の形態1)

先ず、本発明の実施の形態1の録画装置および再生装置の構成を述べる。

【0026】

図1に、本発明の実施の形態1の録画装置および再生装置のブロック図を示す。本発明の実施の形態1の録画装置は、第1鍵発生手段6と、記録スクランブル手段7と、第2鍵発生手段8と、KcFIFO9と、鍵暗号化手段10と、対応関係情報生成手段11と、MUX12から構成される。また、本発明の実施の形態1の再生装置は、第2DMUX13と、暗号化鍵取得手段14と、Kcラッチ手段15と、鍵解読手段16と、再生デスクランブル手段17から構成される。なお、図1には、受信復調手段1と、第1DMUX2と、EMM解読手段3と、ECM解読手段4と、放送デスクランブル手段5と、映像デコーダ18と、音デコーダ19も表示する。さらに、記録媒体としてのビデオテープ20と、映像を表示し、音を出力するディスプレイ21も表示する。

【0027】

受信復調手段1は、放送局からの、デジタルの映像データ、音データ、EMM(個別情報)、ECM(番組情報)および暗号化された放送スクランブル鍵Ksを通信衛星を介して入力し、それらの全部または一部の信号波形を整形する手

段である。

【0028】

なお、受信復調手段1が入力する映像データおよび音データは、放送スクランブル鍵K_sによりスクランブルされたデータである。また、以下では、映像データと音データの両方を意味する場合、映像データおよび音データをAVデータとする。

【0029】

また、受信復調手段1が入力するEMM（個別情報）は、後に説明するワーク鍵K_wという鍵を生成するさいに必要となる情報である。

【0030】

さらに、受信復調手段1が入力するECM（番組情報）は、暗号化された放送スクランブル鍵K_sを復元するさいに必要となる情報である。

【0031】

さて、第1DMUX2は、受信復調手段1からの、波形整形された映像データ、音データ、EMM、ECMおよび暗号化された放送スクランブル鍵K_sを分離する手段であるとともに、放送デスクランブル手段5からの、デスクランブルされた映像データおよび音データを分離する手段である。また、第1DMUX2は、再生デスクランブル手段17からの映像データおよび音データを分離する手段でもある。

【0032】

EMM解読手段3は、ユーザID鍵K_mを入力するとともに、第1DMUX2からのEMMを入力し、ユーザID鍵K_mでEMMを解読してワーク鍵K_wを生成する手段である。

【0033】

ECM解読手段4は、EMM解読手段3からのワーク鍵K_wを入力するとともに、第1DMUX2からのECMおよび暗号化された放送スクランブル鍵K_sを入力し、ワーク鍵K_wでECMを解読して放送スクランブル鍵K_sを復元する手段である。

【0034】

放送デスクランブル手段5は、ECM解読手段4からの放送スクランブル鍵Ksを入力するとともに、第1DMUX2からの、スクランブルされたAVデータを入力し、放送スクランブル鍵Ksで、スクランブルされたAVデータをデスクランブルする手段である。

【0035】

第1鍵発生手段6は、放送デスクランブル手段5によってデスクランブルされたAVデータを、再度スクランブルするための記録スクランブル鍵Kssを発生する手段である。

【0036】

記録スクランブル手段7は、放送デスクランブル手段5からのAVデータを入力するとともに、第1鍵発生手段6からの記録スクランブル鍵Kssを入力し、その記録スクランブル鍵KssでAVデータをスクランブルする手段である。なお、以下では、記録スクランブル鍵KssによりスクランブルされたAVデータをKss(AVデータ)とする。

【0037】

第2鍵発生手段8は、第1鍵発生手段6が発生した記録スクランブル鍵Kssを暗号化するための暗号化鍵Kcを発生する手段である。なお、第2鍵発生手段8は、毎日異なる暗号化鍵Kcを発生するものとし、それら異なるKcをそれぞれKc1、Kc2、Kc3、…とする。また、暗号化鍵Kc1、Kc2、Kc3、…それぞれは、1週間で廃棄されるものであるとする。

【0038】

KcFIFO9は、第2鍵発生手段8からの暗号化鍵Kc1、Kc2、Kc3、…を入力し格納する手段であるとともに、タイマーを有していて、そのタイマーを利用して、入力後1週間経過した暗号化鍵Kcを廃棄する、ファーストインファースアウト機能を有する手段である。

【0039】

鍵暗号化手段10は、第1鍵発生手段6からの記録スクランブル鍵Kssを入力するとともに、KcFIFO9からの暗号化鍵Kcを入力し、その暗号化鍵Kcで記録スクランブル鍵Kssを暗号化する手段である。なお、以下では、暗号

化鍵Kcにより暗号化された記録スクランブル鍵KssをKc(Kss)とする。

【0040】

対応関係情報生成手段11は、記録スクランブル鍵KssによりスクランブルされたAVデータと、その記録スクランブル鍵Kssを暗号化した暗号化鍵Kcとを対応付けるための情報として、暗号化鍵Kc4が発生された日時の情報を生成する手段である。

【0041】

MUX12は、記録スクランブル手段7からのKss(AVデータ)と、鍵暗号化手段10からのKc(Kss)と、対応関係情報生成手段11からの日時情報とを入力し、それらをビデオテープ20に記録する手段である。

【0042】

第2DMUX13は、ビデオテープ20に記録された、Kss(AVデータ)、Kc(Kss)および日時情報を入力し、それらを分離する手段である。

【0043】

暗号化鍵取得手段14は、第2DMUX13からの日時情報を入力し、その日時情報に基づいて、再生しようとするKss(AVデータ)に対応する暗号化鍵Kcを特定し、その特定した暗号化鍵KcをKcFIFO9のなかから取得する手段である。

【0044】

Kcラッチ手段15は、暗号化鍵取得手段14からの暗号化鍵Kcを入力してラッチし、鍵解読手段16に出力する手段である。

【0045】

鍵解読手段16は、第2DMUX13からのKc(Kss)を入力するとともに、Kcラッチ手段15からの暗号化鍵Kcを入力し、その暗号化鍵KcでKc(Kss)を解読し、記録スクランブル鍵Kssを復元する手段である。

【0046】

再生デスクランブル手段17は、第2DMUX13からのKss(AVデータ)を入力するとともに、鍵解読手段16からの記録スクランブル鍵Kssを入力

し、その記録スクランブル鍵 K_{ss} で K_{ss} (AVデータ) をデスクランブルする手段である。

【0047】

映像デコーダ 18 は、第 1 DMUX 2 からの映像データを復号する手段である。

【0048】

音デコーダ 19 は、第 1 DMUX 2 からの音データを復号する手段である。

【0049】

なお、請求項 1 の本発明の、スクランブル手段として記録スクランブル手段 7、暗号化鍵発生手段として第 2 鍵発生手段 8、格納手段として K_{cFIFO} 9、鍵暗号化手段として鍵暗号化手段 10、対応関係情報生成手段として対応関係情報生成手段 11、記録手段として MUX 12 を用いた。また、請求項 6 の本発明のスクランブル鍵発生手段として第 1 鍵発生手段 6 を、本実施の形態では用いた。さらに、請求項 7 の本発明の、暗号化鍵取得手段として暗号化鍵取得手段 14、鍵暗号化解読手段として鍵解読手段 16、スクランブル解除手段として再生デスクランブル手段 17 を用いた。

【0050】

次に、このような本発明の実施の形態 1 の録画装置の動作を述べる。

【0051】

まず、受信復調手段 1 は、放送局からの、デジタルの映像データ、音データ、EMM (個別情報)、ECM (番組情報) および暗号化された放送スクランブル鍵 K_s を入力し、映像データおよび音データの信号波形の乱れを整形し、映像データ、音データ、EMM、ECM および暗号化された放送スクランブル鍵 K_s を第 1 DMUX 2 に出力する。

【0052】

その後、第 1 DMUX 2 は、受信復調手段 1 からの映像データ、音データ、EMM、ECM および放送スクランブル鍵 K_s を入力して分離し、映像データおよび音データ (AVデータ) を放送デスクランブル手段 5 に出力する。また、EMM を EMM 解読手段 3 に出力し、ECM および暗号化された放送スクランブル鍵

KsをECM解読手段4に出力する。

【0053】

次に、EMM解読手段3は、ユーザID鍵Kmを入力するとともに、第1DMUX2からのEMMを入力し、ユーザID鍵KmでEMMを解読してワーク鍵Kwを生成し、ECM解読手段4に出力する。

【0054】

さらに、ECM解読手段4は、EMM解読手段3からのワーク鍵Kwを入力するとともに、第1DMUX2からの、ECMおよび暗号化された放送スクランブル鍵Ksを入力し、ワーク鍵KwでECMを解読して、暗号化された放送スクランブル鍵Ksの暗号化を復元し、放送デスクランブル手段5に出力する。

そして、放送デスクランブル手段5は、ECM解読手段4からの放送スクランブル鍵Ksを入力するとともに、第1DMUX2からの、スクランブルされたAVデータを入力し、放送スクランブル鍵Ksで、スクランブルされたAVデータをデスクランブルする。そして、放送デスクランブル手段5は、デスクランブルされたAVデータを第1DMUX2または記録スクランブル手段7に出力する。なお、放送デスクランブル手段5は、リアルタイムでAVデータを直接ディスプレイ21に表示させる場合に第1DMUX2に出力し、ビデオテープ20にAVデータを記録させる場合に記録スクランブル手段7に出力する。ただし、ビデオテープ20に記録されるAVデータは、放送デスクランブル手段5からの、そのままのAVデータではなく、再度スクランブルされたデータである。

【0055】

はじめに、放送デスクランブル手段5がAVデータを第1DMUX2に出力する場合について説明する。

【0056】

その場合、第1DMUX2は、放送デスクランブル手段5からのAVデータ入力し、それを映像データと音データに分離して、映像データを映像デコーダ18に出力し、音データを音デコーダ19に出力する。その後、映像デコーダ18および音デコーダ19それぞれは、第1DMUX2からの映像データまたは音データを復号し、ディスプレイ21に出力する。そして、ディスプレイ21は、映像

を表示し音を出力する。

【0057】

次に、放送デスクランブル手段5がAVデータを記録スクランブル手段7に出力する場合について説明する。つまり、上述したように、ビデオテープ20にAVデータを記録する場合である。

【0058】

まず、記録スクランブル手段7は、放送デスクランブル手段5からの、デスクランブルされたAVデータを入力する。

【0059】

そして、第1鍵発生手段6は、記録スクランブル手段7が入力したAVデータをスクランブルするための記録スクランブル鍵Kssを発生し、記録スクランブル手段7および鍵暗号化手段10に出力する。

【0060】

次に、記録スクランブル手段7は、第1鍵発生手段6からの記録スクランブル鍵Kssを入力し、その記録スクランブル鍵KssでAVデータをスクランブルする。つまり、Kss(AVデータ)を生成する。そして、Kss(AVデータ)を対応関係情報生成手段11およびMUX12に出力する。

【0061】

他方、第2鍵発生手段8は、第1鍵発生手段6が発生した記録スクランブル鍵Kssを暗号化するための暗号化鍵Kcを発生する。その第2鍵発生手段8が発生する暗号化鍵Kcは毎日異なるものとする。ここでは、以下の説明の便宜上、録画装置が動作し始める日を1998年1月1日であるとし、記録時である本日をその日から3日後の1998年1月4日であるとし、図2の暗号化鍵Kcリスト(a)に示すように、1月1日に発生された暗号化鍵KcをKc1、1月2日に発生された暗号化鍵KcをKc2、…、1月4日に発生された暗号化鍵KcをKc4とする。また、以下、同様にして暗号化鍵Kcは発生されるものとする。なお、ことわりがない限り、以下、1月4日の録画装置の動作について説明する。

【0062】

さて、KcFIFO9は、図2(a)のリストに示すように、1月1日から毎日一つづつの暗号化鍵Kcを第2鍵発生手段8から既に入力して格納し、1月3日までに暗号化鍵Kc1、Kc2、Kc3を格納しておき、本日1月4日には、Kc4を入力して格納する。その格納は、常に最新の暗号化鍵Kcが図2(a)のリストのトップの順位にくるように行われ、また、古いものは順次順位を下げるように行われる。なお、KcFIFO9は、格納した暗号化鍵Kc1、Kc2、…を、それぞれの格納から1週間経過した後に廃棄する。例えば、図2(b)のリストに示すように、1月9日になると、Kc1、Kc2という暗号化鍵は廃棄され、KcFIFO9は、Kc9、Kc8、…、Kc4、Kc3という順序で7つの暗号化鍵を格納することになる。つまり、KcFIFO9が格納する暗号化鍵Kcの数は7までである。

【0063】

次に、鍵暗号化手段10は、第1鍵発生手段6からの記録スクランブル鍵Kssを入力するとともに、KcFIFO9を介して、第2鍵発生手段8が記録時である1月4日に発生した暗号化鍵Kc4を入力し、その暗号化鍵Kc4で記録スクランブル鍵Kssを暗号化する。つまり、Kc4(Kss)を生成する。

【0064】

そして、対応関係情報生成手段11は、記録スクランブル手段7からのKss(AVデータ)と、鍵暗号化手段10からのKc4(Kss)とを入力し、その暗号化鍵Kc4と、その暗号化鍵Kc4で暗号化された記録スクランブル鍵KssによりスクランブルされたAVデータとを対応付けるための情報として、その暗号化鍵Kc4が発生された日時の情報を生成する。つまり、1月4日という日時情報を生成する。

【0065】

その後、MUX12は、記録スクランブル手段7からのKss(AVデータ)と、鍵暗号化手段10からのKc4(Kss)と、対応関係情報生成手段11からの1月4日という日時情報とを入力し、それらを1組としてビデオテープ20に記録する。

【0066】

このようにして、毎日、その日に発生された暗号化鍵 K_{cn} ($n=1, 2, \dots$) に対応する K_{cn} (K_{ss}) と、 K_{ss} (AVデータ) と、その日の日時情報とが1組となってビデオテープ20に記録される。

【0067】

次に、本発明の実施の形態1の再生装置の動作を述べる。

【0068】

つまり、録画装置によってビデオテープ20に記録された K_{ss} (AVデータ) を再生する場合について説明する。

【0069】

以下の説明の便宜上、再生装置がビデオテープ20の K_{ss} (AVデータ) を再生する日を1月9日であるとする。そして、再生装置は、1月1日にビデオテープ20に記録された K_{ss} (AVデータ) と、1月3日にビデオテープ20に記録された K_{ss} (AVデータ) とを再生しようとするものとする。

【0070】

はじめに、再生装置が1月1日にビデオテープ20に記録された K_{ss} (AVデータ) を再生しようとする場合について説明する。

【0071】

まず、第2DMUX13は、ビデオテープ20からの、1月1日に記録された K_{ss} (AVデータ) と、 K_{c1} (K_{ss}) と、1月1日という日時情報とを入力し、それらを分離し、1月1日という日時情報を暗号化鍵取得手段14に出力する。

【0072】

そして、暗号化鍵取得手段14は、その1月1日という日時情報を入力し、その日時情報に基づいて、暗号化鍵 K_{c1} を特定し、 K_{cFIFO9} が格納している、図2(b)のリストのなかから暗号化鍵 K_{c1} を検索する。しかしながら、その暗号化鍵 K_{c1} は、発生から一週間以上経過しているので、 K_{cFIFO9} により廃棄されており、図2(b)のリストのなかには存在しない。したがって、暗号化鍵取得手段14は、暗号化鍵 K_{c1} を取得することができない。その結果、再生デスクランブル手段17は、その暗号化鍵 K_{c1} を間接的に用いてデス

クランブルする必要がある、1月1日に記録されたK s s (A Vデータ) をデスクランブルすることができなくなり、そのA Vデータがディスプレイ21に出力されても、解読不能なため、ディスプレイ21は、A Vデータ本来の映像および音を出力することができない。

【0073】

次に、再生装置が1月3日にビデオテープ20に記録されたK s s (A Vデータ) を再生しようとする場合について説明する。

【0074】

まず、第2 DMUX 13は、ビデオテープ20からの、1月3日に記録されたK s s (A Vデータ) と、K c 3 (K s s) と、1月3日という日時情報とを入力し、それらを分離し、1月3日という日時情報を暗号化鍵取得手段14に出力する。

【0075】

次に、暗号化鍵取得手段14は、その1月3日という日時情報を入力し、その日時情報に基づいて、暗号化鍵K c 3を特定し、K c F I F O 9が格納している、図2 (b) のリストのなかから暗号化鍵K c 3を検索してその暗号化鍵K c 3を取得し、それをK c ラッチ手段15に出力する。

【0076】

その後、K c ラッチ手段15は、暗号化鍵K c 3を入力し、鍵解読手段16に出力する。また、第2 DMUX 13は、K c 3 (K s s) を鍵解読手段16に出力する。

【0077】

そして、鍵解読手段16は、第2 DMUX 13からのK c 3 (K s s) を入力するとともに、K c ラッチ手段15からの暗号化鍵K c 3を入力し、その暗号化鍵K c 3でK c 3 (K s s) を解読し、記録スクランブル鍵K s sを復元して、その記録スクランブル鍵K s sを再生デスクランブル手段17に出力する。また、第2 DMUX 13は、K s s (A Vデータ) を鍵解読手段16に出力する。

【0078】

次に、再生デスクランブル手段17は、第2 DMUX 13からのK s s (A V

データ)を入力するとともに、鍵解読手段16からの記録スクランブル鍵Kssを入力し、その記録スクランブル鍵KssでKss(AVデータ)をデスクランブルして、そのデスクランブルされたAVデータを第1DMUX2に出力する。

【0079】

そして、第1DMUX2は、再生デスクランブル手段17からのAVデータを入力し、それを映像データと音データに分離して、映像データを映像デコーダ18に出力し、音データを音デコーダ19に出力する。その後、映像デコーダ18および音デコーダ19それぞれは、第1DMUX2からの映像データまたは音データを復号し、ディスプレイ21に出力する。そして、ディスプレイ21は、映像を表示し音を出力する。

【0080】

このようにして、ビデオテープ20に記録されたKss(AVデータ)それぞれは、記録されてから1週間以内でないと、最終的に、本来の映像および音声として再生されない。

【0081】

なお、上述した実施の形態1では、ビデオテープ20に記録されたKss(AVデータ)それぞれは、記録されてから1週間以内であれば再生されるとしたが、1週間以内というような期間の制限ではなく、Kss(AVデータ)それぞれの再生回数を、例えば1回や3回というように制限して、その制限再生回数以内でないと、再生されないとしてもよい。つまり、図3に示すように、本発明の再生装置がカウンタ22を備え、そのカウンタ22が各Kss(AVデータ)の再生回数をチェックし、例えば1回や3回というような制限された再生回数に達した場合、KcFIFO9が、そのKss(AVデータ)に対応する暗号化鍵Kcを廃棄するとしてもよい。また、上述した1週間以内というような期間の制限と再生回数の制限を併用するとしてもよい。

【0082】

また、上述した実施の形態1では、KcFIFO9は、格納した暗号化鍵Kcを1週間経過した後に廃棄するとした。しかし、KcFIFO9は、格納した暗号化鍵Kcを1週間経過しても廃棄せずに、格納したままにしておき、暗号化鍵

取得手段 14 が、 K_{ss} (AVデータ) を再生しようとする日が暗号化鍵 K_c の発生から 1 週間以内か否かを判断して、または、制限回数内か否かを判断して、1 週間以内または制限回数内以内であれば、再生しようとする K_{ss} (AVデータ) に対応する暗号化鍵 K_c を K_c FIFO9 から取得できるとしてもよい。したがって、この場合、請求項 8 の本発明では、スクランブル手段として記録スクランブル手段 7、暗号化鍵発生手段として第 2 鍵発生手段 8、格納手段として K_c FIFO9、鍵暗号化手段として鍵暗号化手段 10、対応関係情報生成手段として対応関係情報生成手段 11、記録手段として MUX12 がそれぞれ該当することになる。また、請求項 12 の本発明では、暗号化鍵取得手段として暗号化鍵取得手段 14、鍵暗号化解読手段として鍵解読手段 16、スクランブル解除手段として再生デスクランブル手段 17 がそれぞれ該当することになる。

【0083】

また、上述した実施の形態 1 では、第 1 鍵発生手段 6 は、記録スクランブル手段 7 が入力した AV データをスクランブルするための記録スクランブル鍵 K_{ss} を発生するとした。しかし、本発明の録画装置は、図 4 に示すように、第 1 鍵発生手段 6 を備えず、記録スクランブル手段 7 は、放送局から送られてくる放送スクランブル鍵 K_s を、放送デスクランブル手段 5 を介して入力し、その放送スクランブル鍵 K_s で、または、その放送スクランブル鍵 K_s を加工したもので、AV データをスクランブルするとしてもよい。その場合、鍵暗号化手段 10 は、記録スクランブル手段 7 から、放送スクランブル鍵 K_s 、または、その放送スクランブル鍵 K_s を加工したものを入力し、それを暗号化鍵 K_c で暗号化する。

【0084】

また、上述した実施の形態 1 では、記録スクランブル手段 7 は、第 1 鍵発生手段 6 からの記録スクランブル鍵 K_{ss} で AV データをスクランブルするとした。しかし、本発明の録画装置は、図 5 に示すように、第 1 鍵発生手段 6、鍵暗号化手段 10 を備えず、記録スクランブル手段 7 は、第 2 鍵発生手段 8 からの暗号化鍵 K_c を K_c FIFO9 を介して入力し、その暗号化鍵 K_c を記録スクランブル鍵 K_c として使用し、その記録スクランブル鍵 K_c により、AV データをスクランブルするとしてもよい。この場合、ビデオテープ 20 には、記録スクランブル

鍵KcによりスクランブルされたAVデータ、つまり、Kc（AVデータ）と、記録スクランブル鍵Kcとが記録される。またその場合、本発明の再生装置は、図5に示すように、鍵解読手段16を備えないことになる。したがって、Kc（AVデータ）を再生しようとする場合、スクランブル鍵取得手段23は、対応する記録スクランブル鍵Kcを特定し、それをKcFIFO9のなかから取得する。そして、再生デスクランブル手段17は、ビデオテープ20からのKc（AVデータ）を第2DMUX13を介して入力するとともに、スクランブル鍵取得手段23からの記録スクランブル鍵KcをKcラッチ手段15を介して入力し、その記録スクランブル鍵KcでKc（AVデータ）をデスクランブルする。そのため、この場合、つまり、請求項15および20の本発明では、スクランブル鍵発生手段として第2鍵発生手段8、格納手段としてKcFIFO9、スクランブル手段として記録スクランブル手段7、対応関係情報生成手段として対応関係情報生成手段11、記録手段として第1DMUX2がそれぞれ該当することになる。また、請求項19および22の本発明では、スクランブル鍵取得手段としてスクランブル鍵取得手段23、スクランブル解除手段として再生デスクランブル手段17がそれぞれ該当することになる。

【0085】

また、上述した実施の形態1の録画装置は、図6に示すように、課金手段24を備え、ビデオテープ20にKss（AVデータ）を記録するさい、その記録に対する所定の課金をユーザに課し、あらかじめユーザから所定の料金が放送局等に支払われた場合、もしくは、少なくとも記録するさいに所定の料金が支払われた場合のみ、Kss（AVデータ）はビデオテープ20に記録されるとしてもよい。また、課金手段24は、図6に示す位置に配置されなくとも、鍵暗号化手段10とMUX12との間に配置されるとしてもよい。要するに、課金手段24は、ビデオテープ20にKss（AVデータ）を記録するさい、その記録に対する所定の課金をユーザに課すものでありさえすればよく、配置場所はどの場所であってもよい。

【0086】

また、上述した実施の形態1では、暗号化鍵Kcそれぞれは、発生から1週間

経過すると廃棄されるとしたが、廃棄される日時は、発生から1週間経過後に限定することではなく、1日経過後であっても、3日経過後であっても、または、12時間経過後であってもよい。要するに、暗号化鍵Kcそれぞれは、発生から所定の期間経過すると廃棄されさえすればよい。

【0087】

また、上述した実施の形態1では、第2鍵発生手段8は、毎日、1つつ異なる暗号化鍵Kcを発生するとしたが、第2鍵発生手段8は、同じ日であっても、数時間毎に異なる暗号化鍵Kcを発生するとしてもよい。さらに、ビデオテープ20に所定の番組のKss(AVデータ)を記録する毎に暗号化鍵Kcを発生するとしてもよい。つまり、一回の録画開始からその録画の終了毎に、その都度、暗号化鍵Kcを発生するとしてもよい。要するに、第2鍵発生手段8は、記録しようとするKss(AVデータ)の記録スクランブル鍵Kssを暗号化するための暗号化鍵Kcを発生しさえすればよい。

【0088】

また、上述した実施の形態1では、本発明の対応関係情報として、暗号化鍵Kcが発生されたさいの日時情報を用いたが、本発明の対応関係情報は、記録スクランブル手段7がAVデータを入力した日時、記録スクランブル手段7が記録スクランブル鍵KssでAVデータをスクランブルした日時、第2鍵発生手段8が暗号化鍵Kcを発生した日時、KcFIFO9が暗号化鍵Kcを格納した日時、鍵暗号化手段10が暗号化鍵Kcで記録スクランブル鍵Kssを暗号化した日時、または、MUX12がビデオテープ20にKss(AVデータ)を記録した日時の情報であってもよい。もしくは、上述した暗号化鍵Kcが発生されたさいの日時や、記録スクランブル手段7がAVデータを入力した日時等と、AVデータを再生しようとする日時との情報であってもよい。その場合、図2の暗号化鍵Kcリストの各暗号化鍵Kcが毎日順位を下げることに基づいて、また、2つの日時の差が考慮されて、暗号化鍵Kcが取得されることになる。または、本発明の対応関係情報は、上述した暗号化鍵Kcが発生されたさいの日時や、記録スクランブル手段7がAVデータを入力した日時等と、AVデータを再生しようとする日時とに基づき、また、図2の暗号化鍵Kcリストの各暗号化鍵Kcが毎日順位

を下げる事が考慮された、図2の暗号化鍵Kcリストの番号情報等であってもよい。

【0089】

また、上述した実施の形態1では、記録媒体としてのビデオテープ20を用いたが、記録媒体は、ビデオテープ20に限らず、ハードディスクであってもよい。

【0090】

また、上述した実施の形態1では、第1鍵発生手段6はAVデータをスクランブルするための記録スクランブル鍵Kssを発生するが、その記録スクランブル鍵Kssは、簡単に解読することができないように、例えば数十秒などの短い期間で更新されるとしてもよい。

【0091】

さらに、上述した録画装置または再生装置は、暗号化鍵Kcの発生から例えば1週間という所定の期間を経過するなどして、その暗号化鍵Kcが廃棄されたり、使用不可になる前に、その暗号化鍵Kcに対応するKss（AVデータ）が一度も再生されていない場合、その旨の情報をユーザに通知する手段を備えてもよい。

【0092】

【発明の効果】

以上説明したところから明らかなように、本発明は、AVデータを記録媒体に記録し、そのAVデータの有効再生期間や有効再生回数の制限を遵守する録画装置および再生装置を提供することができる。

【図面の簡単な説明】

【図1】

本発明の実施の形態1の録画装置および再生装置のブロック図

【図2】

本発明の実施の形態1の録画装置および再生装置に使用される暗号化鍵Kcリストの一例を示す図

【図3】

図 1 とは異なる本発明の録画装置および再生装置のブロック図

【図 4】

図 1 または 3 とは異なる本発明の録画装置および再生装置のブロック図

【図 5】

図 1、3 または 4 とは異なる本発明の録画装置および再生装置のブロック図

【図 6】

図 1、3、4 または 5 とは異なる本発明の録画装置および再生装置のブロック

図

【図 7】

従来の録画再生装置のブロック図

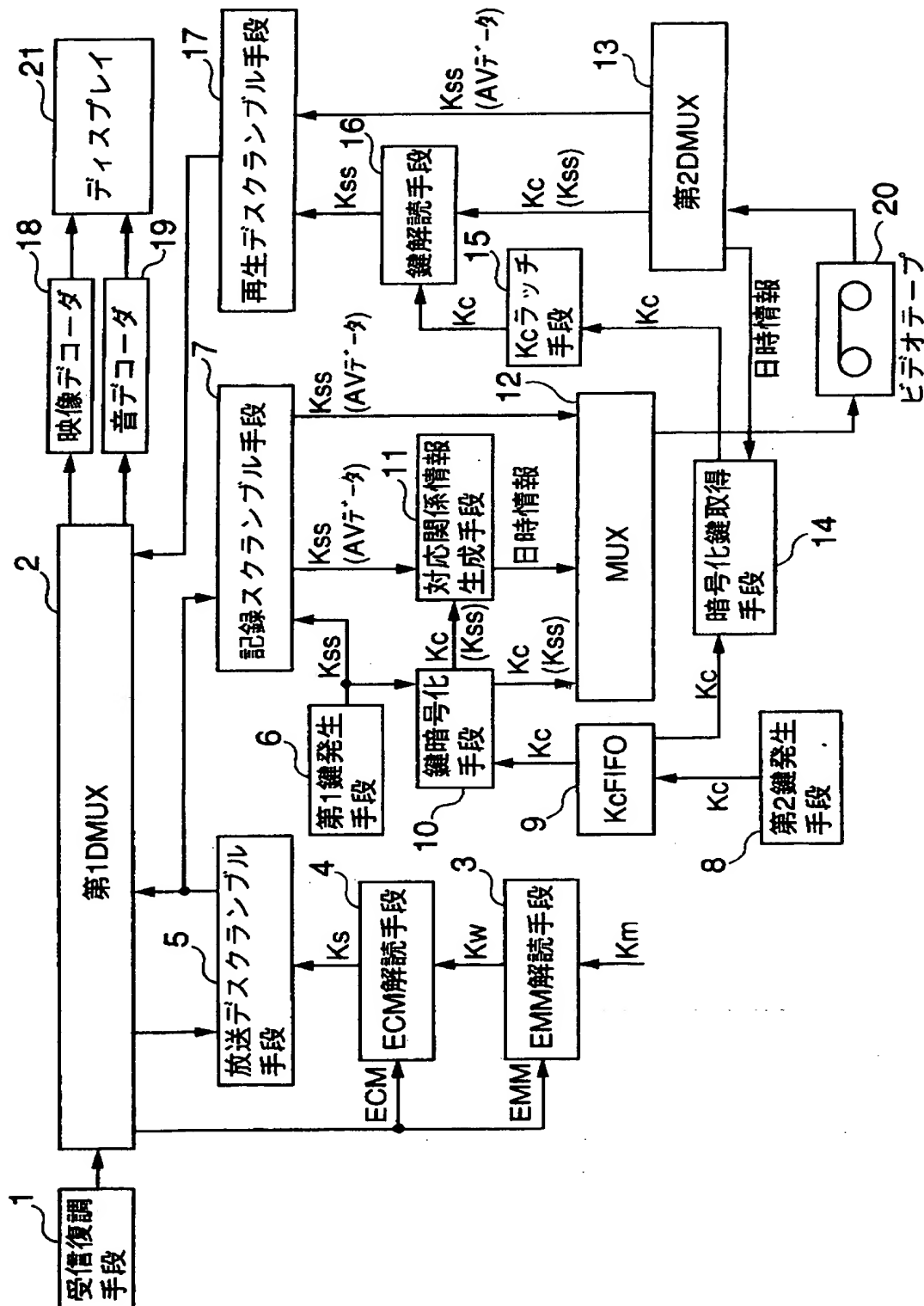
【符号の説明】

- 1 受信復調手段
- 2 第 1 DMUX
- 3 EMM 解読手段
- 4 ECM 解読手段
- 5 放送デスクランブル手段
- 6 第 1 鍵発生手段
- 7 記録スクランブル手段
- 8 第 2 鍵発生手段
- 9 Kc FIFO
- 10 鍵暗号化手段
- 11 対応関係情報生成手段
- 12 MUX
- 13 第 2 DMUX
- 14 暗号化鍵取得手段
- 15 Kc ラッチ手段
- 16 鍵解読手段
- 17 再生デスクランブル手段
- 18 映像デコーダ

- 19 音デコーダ
- 20 ビデオテープ
- 21 ディスプレイ
- 22 カウンタ
- 23 スクランブル鍵取得手段
- 24 課金手段

【書類名】 図面

【図 1】



【図2】

暗号化鍵 Kc リスト

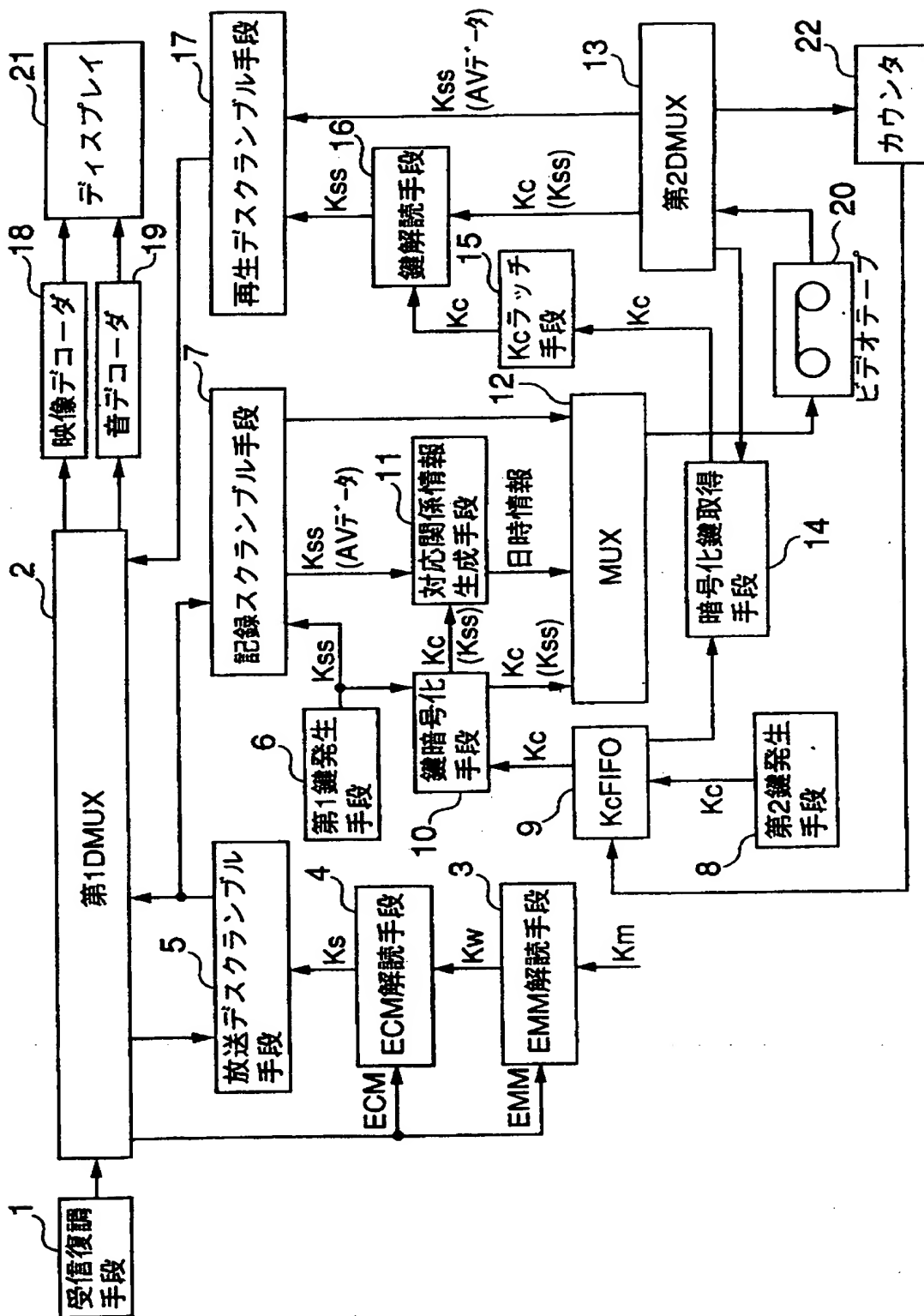
(a) 1月4日現在

No.	暗号化鍵	鍵発生日
1	Kc4	1月4日
2	Kc3	1月3日
3	Kc2	1月2日
4	Kc1	1月1日
5		
6		
7		

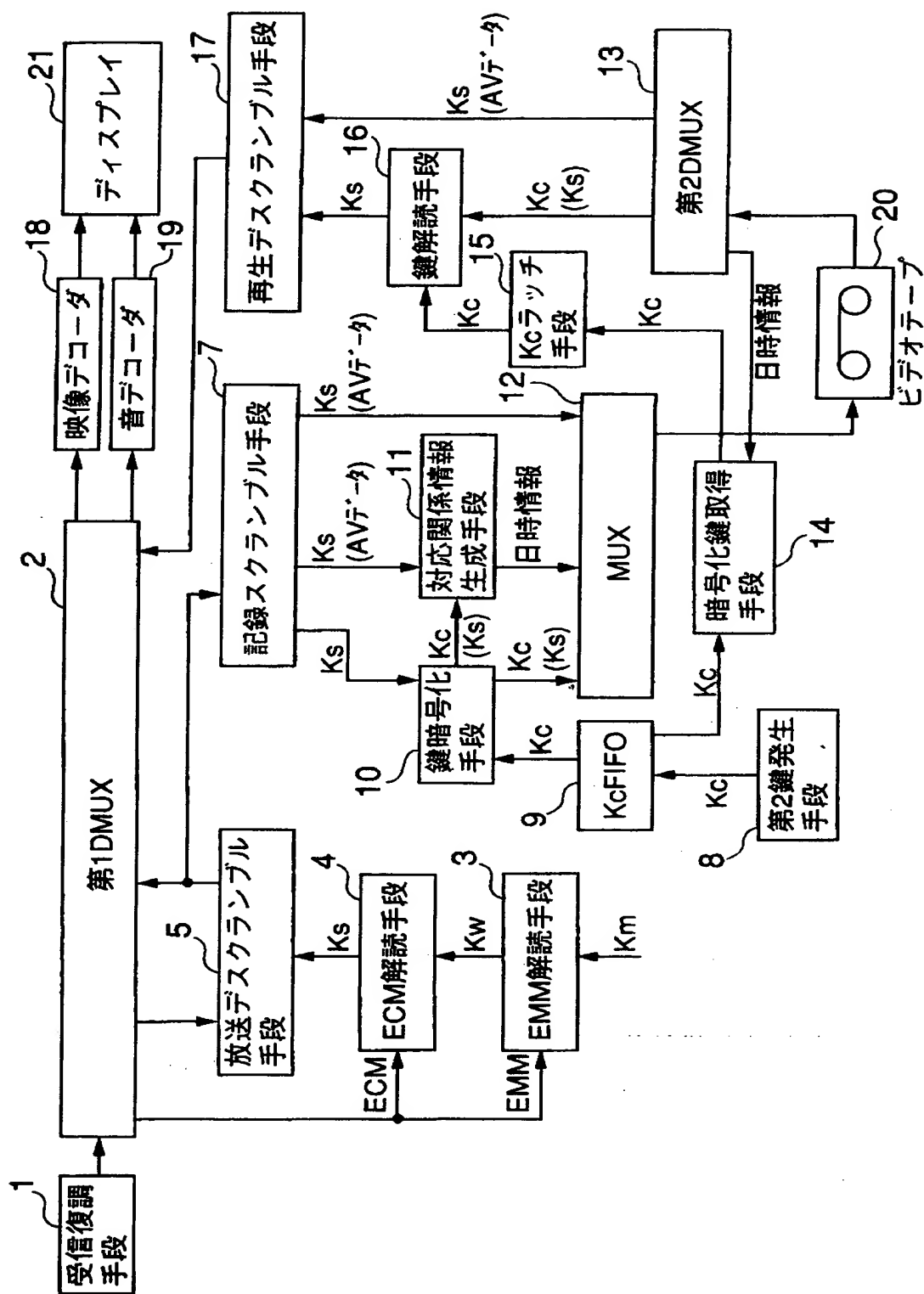
(b) 1月9日現在

No.	暗号化鍵	鍵発生日
1	Kc9	1月9日
2	Kc8	1月8日
3	Kc7	1月7日
4	Kc6	1月6日
5	Kc5	1月5日
6	Kc4	1月4日
7	Kc3	1月3日

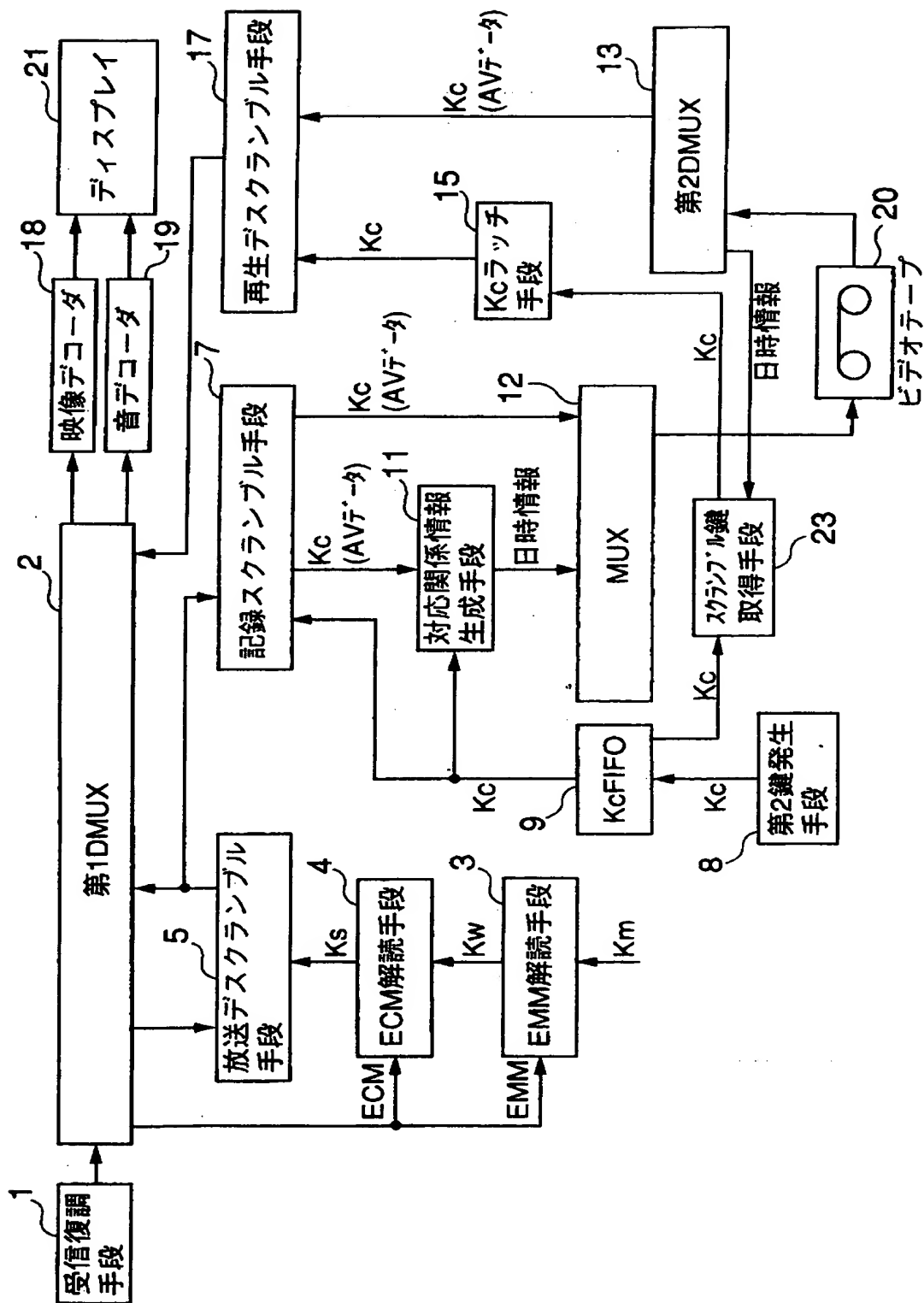
【図3】



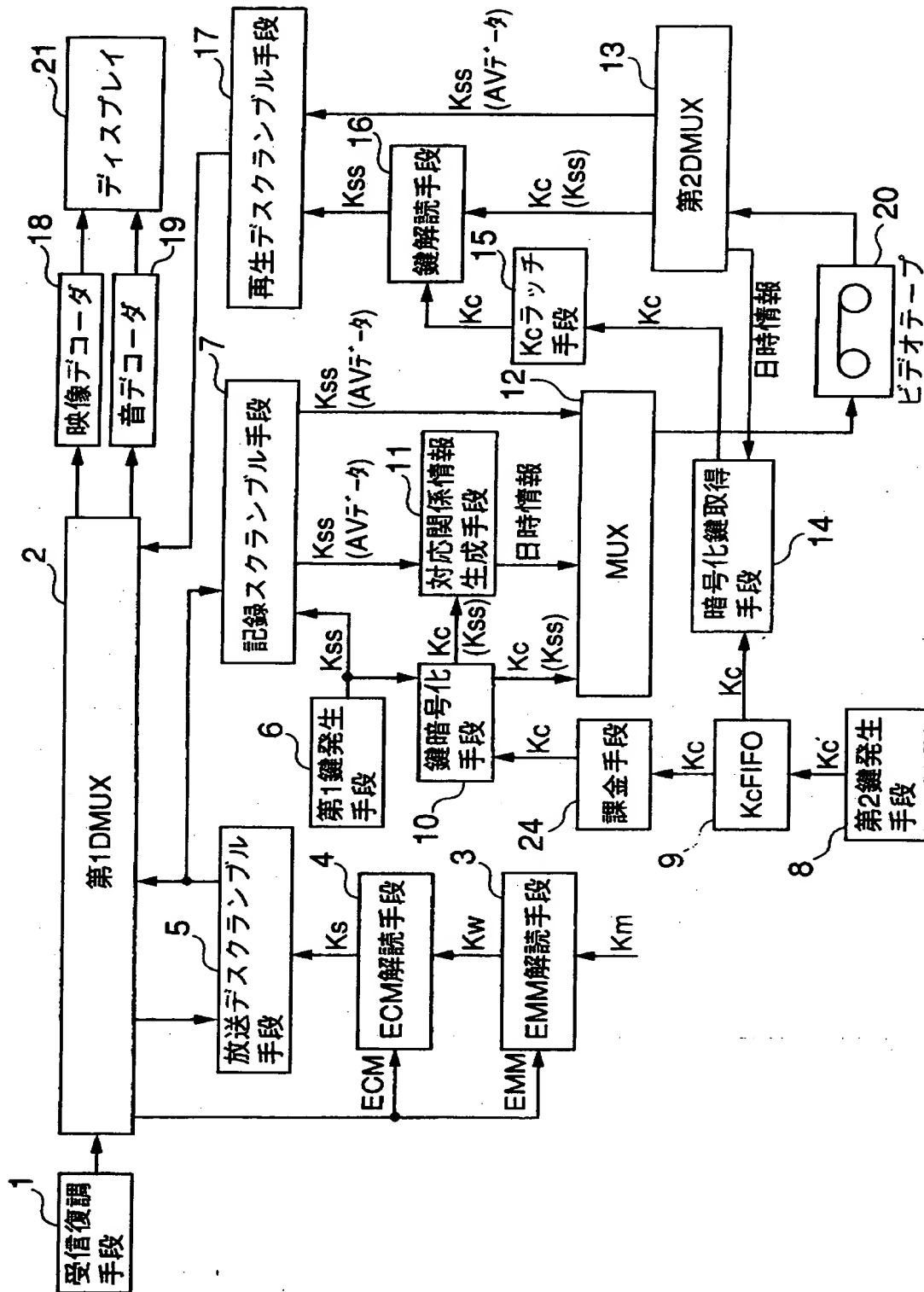
【図4】



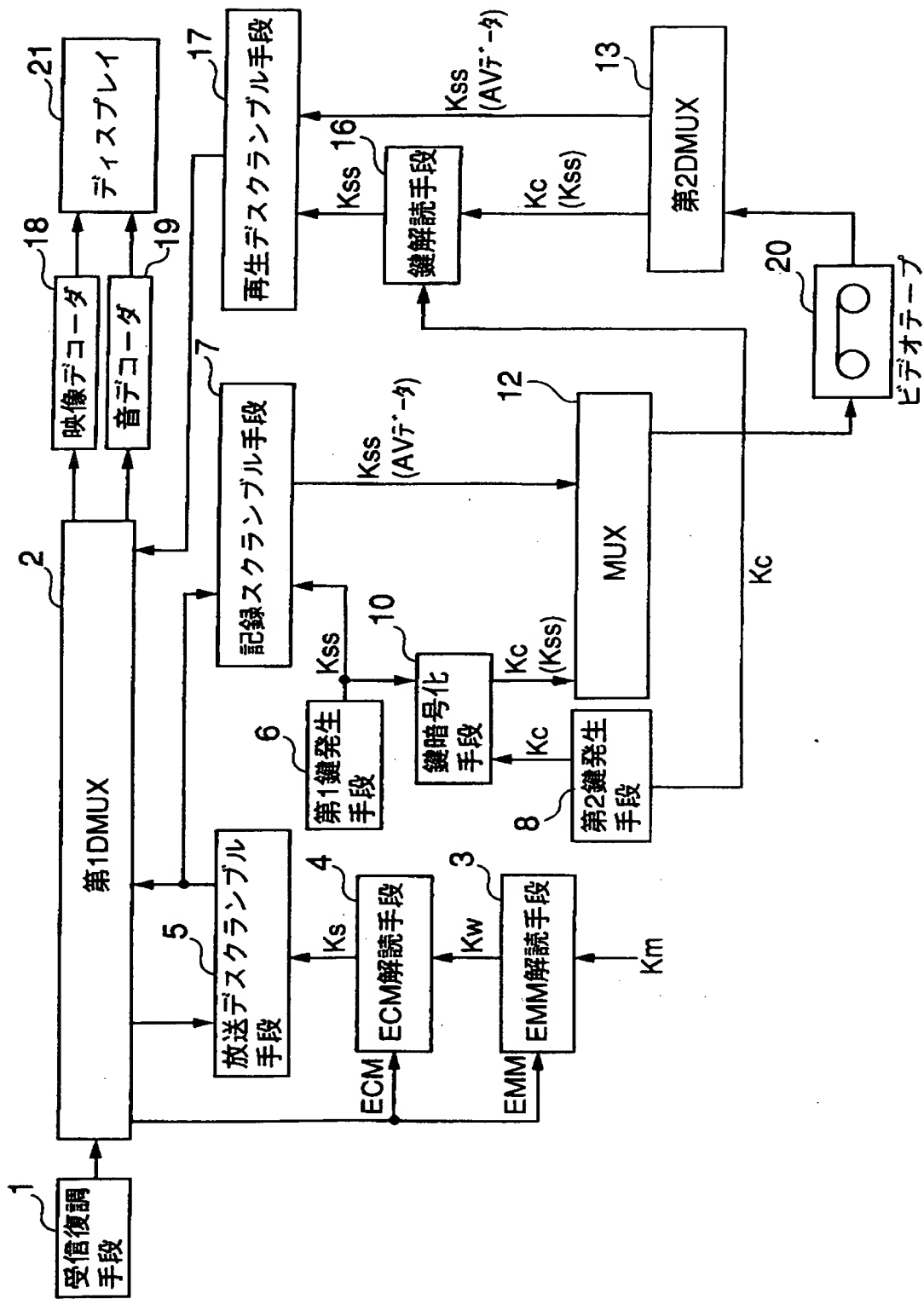
【図 5】



【図6】



【図 7】



【書類名】 要約書

【要約】

【課題】従来の録画再生装置は、A Vデータを記録媒体に記録すると、そのA Vデータの有効再生期間や有効再生回数の制限を守らないという課題があった。

【解決手段】スクランブル鍵K s sでA Vデータをスクランブルする記録スクランブル手段7と、スクランブル鍵K s sを暗号化するための暗号化鍵K cを発生する第2鍵発生手段8と、第2鍵発生手段8からの暗号化鍵K cを格納し、その後、その暗号化鍵K cが所定の条件に合えば、その暗号化鍵K cを消去するK c F I F O 9と、暗号化鍵K cでスクランブル鍵K s sを暗号化する鍵暗号化手段10と、暗号化鍵K cが発生された日時の情報を生成する対応関係情報生成手段11と、スクランブルされた映像および／または音のデータ、暗号化されたスクランブル鍵K s s、および、日時情報を入力し、それらをビデオテープ20に記録するM U X 1 2とを備える。

【選択図】 図1

【書類名】 職権訂正データ
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】
【識別番号】 000005821
【住所又は居所】 大阪府門真市大字門真 1006 番地
【氏名又は名称】 松下電器産業株式会社
【代理人】 申請人
【識別番号】 100092794
【住所又は居所】 大阪市淀川区宮原 5 丁目 1 番 3 号 新大阪生島ビル
松田特許事務所
【氏名又は名称】 松田 正道

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日	1990年 8月28日
[変更理由]	新規登録
住 所	大阪府門真市大字門真1006番地
氏 名	松下電器産業株式会社